Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-3-2020
January 16, 2020

Heightened Cybersecurity Risk Considerations

Summary: In response to the heightened cybersecurity risk facing the financial services industry and other critical business sectors, the FDIC and the Office of the Comptroller of the Currency issued an interagency statement on heightened cybersecurity risk. The statement focuses on risk management principles that can reduce the risk of a cyber-attack and minimize business disruptions.

Statement of Applicability to Institutions under $1 Billion in Total Assets: This Financial Institution Letter applies to all FDIC-supervised institutions, including community institutions.

Distribution:
FDIC-Supervised Institutions

Suggested Routing:
Chief Executive Officer
Chief Information Officer
Chief Information Security Officer

Related Topics:
Federal Financial Institutions Examination Council Cybersecurity Awareness Resources

Interagency Guidelines Establishing Information Security Programs

Attachment:
Heightened Cybersecurity Risk

Contact:
Donald Saxinger, Chief, IT Supervision, DSaxinger@fdic.gov or (202) 898-3864

Note:
Access FDIC Financial Institution Letters (FILs) on the FDIC's website.

Subscribe to receive FILs electronically.

Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877-275-3342 or 703-562-2200).

Highlights:

- The Department of Homeland Security has indicated there is heightened risk of cyber-attack against U.S. targets because of increased geopolitical tension.
- The current environment provides an opportunity for banks to re-evaluate the adequacy of safeguards to protect against various types of cybersecurity risk.
- The attached *Heightened Cybersecurity Risk* document highlights principles previously articulated by the FDIC and other banking regulators including: business resilience, authentication, system configuration, security tool, data protection, and employee training.
- When banks apply cybersecurity risk management principles and risk mitigation techniques, they reduce the risk of a cyber attack's success and minimize the negative impacts of a disruptive and destructive cyber attack.